NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
NSA/CSS POLICY 1-13

Issue Date: 31 December 2014
Revised:

(U) SECOND PARTY INTEGREES

(U) PURPOSE AND SCOPE

(U//~~FOUO~~) This policy assigns responsibilities and procedures for the establishment of *Second Party Integree* positions and the placement of Second Party Integrees, including personnel involved in military exchange programs, into NSA/CSS. This policy applies to *NSA/CSS Washington*, the *NSA/CSS Extended Enterprise*, and United States Signals Intelligence System tactical locations.

MICHAEL S. ROGERS
Admiral, U.S. Navy
Director, NSA/Chief, CSS

Endorsed by
Associate Director for Policy

(U) DISTRIBUTION:
DP09
DJ1

(U) This Policy 1-13 supersedes NSA/CSS Policy 1-13 dated 16 August 2004.
(U) OPI: Foreign Affairs Directorate, DP, 963-5454s.
(U) No section of this document, regardless of classification, shall be released without approval from the Office of Corporate Policy (DJ1).

(U) POLICY

1. (U//~~FOUO~~) NSA/CSS shall support the integration of *Second Party* personnel into the NSA/CSS workforce throughout the *NSA/CSS Global Cryptologic Enterprise* when it is beneficial to the United States Cryptologic System mission, strengthens relationships with the Second Party nations, and is consistent with U.S. Government law, policy, strategy, and interests. The integration of Second Party personnel into the NSA/CSS workforce must be in compliance with Department of Defense Directive (DoDD) 5230.20, "Visits, Assignments, and Exchanges of Foreign Nationals" (Reference a).

2. (U//~~FOUO~~) Second Party Integrees shall not perform inherently governmental functions, which must remain the responsibility and within the purview of NSA/CSS Government employees.

a. (U//~~FOUO~~) Second Party Integrees shall not be assigned responsibilities that involve direction of NSA/CSS decision-making processes or that include performing activities that require exercise of substantial direction in applying government authority, including binding NSA/CSS to take or not to take some action by contract, policy, or regulation; to make personnel decisions, including hiring functions; or to make financial/resource decisions. Second Party Integrees may not solely represent the corporate interests of NSA/CSS in internal or external meetings or conferences. While Second Party Integrees may occasionally be called upon to contribute unique expertise to such meetings or conferences, this is permissible only if the Second Party Integree is not asked to commit NSA/CSS resources or to represent NSA/CSS in a policymaking capacity.

b. (U//~~FOUO~~) Second Party Integrees may not perform information technology (IT) systems administrative functions or hold privileged user access on NSA/CSS IT systems, with the exception of local administrative privileges in direct support of mission requirements (i.e., a virtual machine or workstation the administrative access to which is expressly required for mission purposes). All Second Party accesses will comply with Intelligence Community Directive (ICD) Number 503, "Information Technology Systems Security Risk Management, Certification and Accreditation" (Reference b), DoDD 8500.01, "Cybersecurity" (Reference c), NSA/CSS Policy 6-3, "NSA/CSS Operational Information Systems Security Policy" (Reference d), and NSA/CSS Policy 6-20, "Second Party Access to NSA/CSS TS/SCI Classified Information Systems" (Reference e). Requests for exception to this paragraph shall be reviewed and endorsed by the Information System Security Officer (ISSO) prior to submission to the NSA/CSS Authorizing Official for decision.

c. (U//~~FOUO~~) Second Party Integrees may be assigned to leadership positions; however, any supervisory responsibilities that are reserved by law or regulation to an officer or employee of the U.S. Government must be performed by the next higher level U.S. supervisor in the management or command chain. This prohibits the Second Party Integree leader from preparing human resource-related documents, including final performance evaluations, making pay decisions, making decisions regarding the employee's advancement to the next pay level or grade, making award decisions, or similar personnel actions, for any subordinate NSA/CSS employee. Second Party Integrees may, however, provide input to a U.S. Government employee's official supervisor concerning these matters. Additionally, access restrictions may prohibit a Second Party Integree in a leadership position from having full access to the specific details and scope of an NSA/CSS employee's most sensitive mission activities.

3. (U//~~FOUO~~) Information necessary for Second Party Integrees to perform their functions shall be shared unless specifically prohibited by NSA/CSS, Director of National Intelligence (DNI), DoD, or Committee on National Security Systems (CNSS) policy, applicable Executive Orders, or U.S. law. Security ramifications associated with Second Party Integrees must be considered before establishing and staffing any Second Party Integree position.

4. (U) Organizations wishing to establish and staff new Second Party Integree positions shall follow the procedures detailed below.

(b)(3)-P.L. 86-36

(U) PROCEDURES

5. (U//~~FOUO~~) Requirements for Second Party Integree positions will be identified within NSA/CSS Directorates, Associate Directorates, the NSA/CSS Chief of Staff organization, or NSA/CSS Extended Enterprise elements. This policy permits informal exchanges between NSA/CSS and Second Party organizations to identify and define those requirements.

6. (U//~~FOUO~~) The gaining organization wishing to establish, extend, or reallocate an integrated position will prepare, coordinate, and formally track the necessary documentation through the Second Party Affairs Office of the Signals Intelligence (SIGINT) Operations Group (DP1), Foreign Affairs Directorate (FAD), and the Associate Directorate for Security & Counterintelligence (ADS&CI) to the appropriate Director, Deputy Director, Associate Director, or NSA/CSS Chief of Staff. Extended Enterprise elements will work through the appropriate governing Headquarters Directorate for review and approval. For SID, the approval authority is in accordance with the SID Delegation of Approval Authorities matrix. The approved package will be returned to FAD for final review and coordination with the affected *Second Party Liaison* Office and subsequent administration of the accountability processes.

7. (U//~~FOUO~~) The appropriate Director, Associate Director, the NSA/CSS Chief of Staff, or a designee may approve waivers to this policy when necessary to effect rapid reallocation of Second Party Integree resources in response to urgent mission requirements.

8. (U) General criteria for establishing and staffing a new Second Party Integree position. (b)(3)-P.L. 86-36

a. (U//~~FOUO~~) NSA/CSS organizations establishing a new Second Party Integree position must first clearly identify and carefully consider the specific mission and associated data needs. *Raw SIGINT data*, intelligence products, or the immediate capability to produce them shall be shared with Integrees only in accordance with DoD, Intelligence Community (IC), NSA/CSS, and SID policy, as appropriate. [redacted] In addition, a Non-Disclosure Agreement (NDA) shall be executed with the Second Party Integree before release of any PROPIN data.

b. (U//~~FOUO~~) There is no minimum assignment length required for a Second Party Integree to obtain an NSANet account. Further, there is no minimum assignment length required for a Second Party Integree to be eligible for access to raw SIGINT data.

c. (U//~~FOUO~~) Second Party personnel who are solely attending NSA/CSS sponsored training are exempt from this policy. However, if access to NSA/CSS networks is a required part of their training, Second Party personnel shall adhere to NSA/CSS Policy 6-20 (Reference e).

d. (U//~~FOUO~~) Security considerations regarding the work-related activities of Second Party Integrees and associated access requirements shall be analyzed, and associated risks mitigated, by the operational element and subject to ADS&CI review and approval, to ensure compliance with information systems, physical, and personnel security policies before establishing and staffing any position.

e. (U//~~FOUO~~) Prior to establishing and staffing a proposed Second Party Integree position, all requirements shall be fully coordinated with the appropriate NSA/CSS offices. New Second Party Integree positions or Second Party Integree assignment extensions must receive prior approval by the head of the organization to which the Integree will be assigned, or by those having specifically delegated approval authority. Second Party Integree reassignment actions shall be coordinated through both the gaining and the losing approval authorities; disagreements will be resolved at the lowest appropriate levels. If the proposed Second Party Integree position will require rotational assignments, such as is required for many developmental programs (e.g., Cryptologic Mathematician Program, Language Analyst Training Program, etc.), each rotational assignment shall be handled as a Second Party Integree reassignment. All appropriate approvals and applicable documentations must be obtained at least 90 days prior (or less,

if agreed to by the gaining and losing approval authorities) to the Second Party Integree beginning the new rotational assignment.

9. (U//~~FOUO~~) In cases where a Second Party Integree will require interaction with any U.S. Government contractor, the U.S. Government contractor will be required to comply with U.S. laws, rules, and regulations, including those governing exports (e.g., the Arms Export Control Act and the International Traffic-In-Arms Regulations (ITAR), 22 CFR 120-130 (Reference f)). The Office of Export Control Policy (DJ3) is the signatory and authority for exemptions. DJ3 identifies the process required for contractors to interact with Second Party Integrees (Reference g).

10. (U) The Office of the General Counsel will advise on any questions regarding whether the integration of Second Party personnel into the NSA/CSS workforce or Second Party use of NSA/CSS capabilities is consistent with the U.S. laws and procedures that govern NSA/CSS activities.

(U) RESPONSIBILITIES

11. (U//~~FOUO~~) Directors, Associate Directors, the NSA/CSS Chief of Staff, and the Extended Enterprise Commanders/Chiefs shall:

a. (U//~~FOUO~~) Identify requirements for Second Party Integree positions and approve assignments, extensions, and reassignments within their respective organizations;

b. (U//~~FOUO~~) Document Second Party Integree requirements for the Second Party Affairs Office (DP1). This documentation shall include the following:

1) (U//~~FOUO~~) A justification stating why establishing a particular Second Party Integree position is necessary or beneficial to either the U.S. cryptologic mission or the Second Party relationship;

2) (U//~~FOUO~~) A description of the specific duties the Second Party Integree will be performing;

3) (U) Affirmation that the level of intelligence and information assurance sharing is consistent with current operational requirements and a statement that lists the security clearances required for the position;

~~(U//FOUO) 4)~~ (U) A statement of information system connectivity or access requirements, including access to [redacted] databases or datasets and access to raw SIGINT data; Integrees into SID will follow SID Management Directive 427, "Access to Data for Second Party Personnel Engaged in SIGINT Production" (Reference h);

(b)(3)-P.L. 36-36

5) (U//~~FOUO~~) A description of the specific procedures that will be instituted within the assigned operational element to prevent the inadvertent disclosure of NOFORN information, information that is releasable to a community of which the Second Party Integree is not a member (for example, REL US/UK information for a Canadian Integree) (hereafter referred to as non-releasable information), or NSA/CSS Special Access Program material (Reference i) unless separate approval has been granted per paragraph 3;

6) (U//~~FOUO~~) Agreement regarding nondisclosure of proprietary or "commercial-in-confidence" information which would otherwise be required or available during a Second Party Integree's tenure. Non-disclosure will be managed within the organization to which the Integree is assigned and an acceptable plan must be in place to prevent the unauthorized and unintended release of PROPIN;

7) (U) Requirements for special training needed by the Second Party Integree, including mandatory intelligence oversight training, other training required of personnel working under DIRNSA/CHCSS SIGINT authority, or National Cryptologic School courses;

8) (U//~~FOUO~~) Assurance that the Second Party parent organization, through the Second Party Liaison Office, maintains security oversight and provides guidance for their assigned Second Party Integree personnel, in coordination with FAD, ADS&CI, and the involved OPI(s);

9) (U//~~FOUO~~)

(b)(3)-P.L. 86-36

10) (U//~~FOUO~~) An acknowledgement of specific, gaining organization responsibilities with regard to the Integree's operational and personnel management needs. The gaining organization accepts responsibility for performing active oversight of the Integree's SIGINT or information assurance (IA) activities. This includes, at a minimum, that the Integree's U.S. supervisor will have an Annual Contribution Evaluation with objectives that require the supervisor to:

a) (U//~~FOUO~~) Keep records of data access, especially non-releasable data; and

b) (U//~~FOUO~~) Perform audits of requisite databases accesses.

c. (U//~~FOUO~~) Coordinate with ADS&CI, the Technology Directorate, and the relevant Oversight and Compliance Organization to assess potential security vulnerabilities for integrating Second Party personnel into a specific operational element;

d. (U//~~FOUO~~) Review the qualifications of, and approve or disapprove, candidates who are nominated to fill Second Party Integree positions. Forward Second Party Integree selections or non-selections to the Second Party Affairs Office (DP1);

(b)(3)-P.L. 86-36

e. (U//~~FOUO~~)

f. (U//~~FOUO~~) Coordinate with the Information Assurance Directorate (IAD) when a Second Party Integree has an Office of Primary Interest (OPI)-approved requirement for access to United States Information Security data, including, but not limited to, IA threat and vulnerability information, U.S. cryptographic algorithms, IA techniques, or U.S. computer security information;

g. (U//~~FOUO~~) Coordinate with the appropriate Information Systems Security Officer and/or Information Systems Security Manager so that appropriate security certification and accreditation documents, risk assessments, and security controls (if required) can be updated before the Second Party Integree arrives for duty and is given access to an information system, in accordance with NSA/CSS Policy 6-20, "Second Party Access to NSA/CSS TS/SCI Classified Information Systems" (Reference e); and

h. (U//~~FOUO~~) Advise the FAD Second Party Affairs Office of any proposed changes in the status of Second Party Integree positions, including rotation, extension, and/or replacement of specific personnel, at least 90 days in advance of the proposed change whenever possible.

12. (U) The Foreign Affairs Director shall:

a. (U//~~FOUO~~) Review all requests for establishing, extending, or reassigning Second Party Integree positions. This includes verifying and endorsing conformance with existing policy and procedures;

b. (U//~~FOUO~~) Coordinate with Second Party Liaison Offices to establish Second Party Integree positions and/or personnel status changes;

c. (U//~~FOUO~~) Advise the requesting operational element of candidates nominated to fill Second Party Integree positions and the dates of availability. Solicit operational element approval(s);

d. (U) Notify the affected Second Party Liaison Office of approvals and

disapprovals of Second Party Integree positions;

e. (U//~~FOUO~~) Advise appropriate organizations when all necessary administrative, security, and personnel actions have been addressed by the responsible offices prior to the arrival or transfer of an individual Second Party Integree;

f. (U//~~FOUO~~) Maintain a current corporate record of all Second Party Integrees at NSAW and the Extended Enterprise, including names, assigned organization, and length of tour; and

g. (U//~~FOUO~~) Ensure that the Second Party parent organization, through the Second Party Liaison Office, provides ADS&CI with clearance certification and relevant background information on a proposed Integree (at a minimum, name, date and place of birth, date of last security background investigation or reinvestigation, citizenship, and citizenship of spouse or "significant other" partner cohabitating with the Integree);

13. (U) The Associate Director for Security and Counterintelligence shall:

a. (U//~~FOUO~~) Review and assess the personnel and physical security vulnerabilities of integrating Second Party personnel into specific NSA/CSS operational element positions and, if appropriate, provide recommendations to mitigate associated risks;

b. (U//~~FOUO~~) Establish individual security records on each Second Party Integree consisting of basic identification, clearance certification status, and current accesses, excluding personal data associated with background/vetting investigations and updates, that remain under the purview of an Integree's home agency;

c. (U//~~FOUO~~) Certify and maintain applicable identification, clearance, and eligibility for access information for all Second Party Integrees;

d. (U) Administer and maintain records of NSA/CSS "Special Access" information granted to Second Party Integrees in accordance with Reference i; and

e. (U) Issue each Second Party Integree the appropriate access token (badge) required for access to NSA/CSS-controlled campuses and buildings in accordance with NSA/CSS Policy 5-7, "NSA/CSS Badge Identification System" (Reference j).

14. (U) The Technology Director, as the NSA/CSS Chief Information Officer, and the NSA/CSS Chief Information Security Officer (CISO) shall:

a. (U//~~FOUO~~) Review and assess the information systems security ramifications of integrating or retaining Second Party personnel within specific NSA/CSS operational element positions;

b. (U//~~FOUO~~) Provide information systems security guidance, in accordance with the requirements of References a, b, and c, to organizations requesting Second Party access to NSA/CSS computer systems or networks and company PROPIN; and

c. (U//~~FOUO~~) Implement and oversee the technical infrastructure that supports digital identity (i.e. Cryptologic Agencies Domain, Reference e) for Second Party Integrees, enabling appropriate identification, authorization, and audit capability for the NSA/CSS TOP SECRET SCI network.

(U) REFERENCES

15. (U) References:

a. (U) DoDD 5230.20, "Visits and Assignments of Foreign Nationals," dated 22 June 2005.

b. (U) ICD 503, "Information Technology Systems Security Risk Management, Certification and Accreditation," dated 15 September 2008. (Intelink)

c. (U) DoDI 8500.01, "Cybersecurity," dated 14 March 2014.

d. (U) NSA/CSS Policy 6-3, "Information Technology Security Authorization Using the Risk Management Framework," dated 7 March 2014.

e. (U) NSA/CSS Policy 6-20, "Second Party Access to NSA/CSS TS/SCI Classified Information Systems," dated 31 March 2014.

f. (U) International Traffic in Arms Regulations (ITAR), 22 CFR 120-130, dated 29 August 2005.

g. (U) NSA/CSS Policy 1-7, "Technology Security Program," dated 24 December 2013.

h. (U) SID Management Directive 427, "Access to Classified U.S. Intelligence Information for Second Party Personnel," dated 28 December 2013.

i (U) NSA/CSS Policy 1-41, "Programs for the Protection of Especially Sensitive Classified Information," dated 7 March 2013 and revised 6 February 2014.

j. (U) NSA/CSS Policy 5-7, "NSA/CSS Badge Identification System," dated 26 October 2007.

k. (U) Executive Order 12333, "United States Intelligence Activities," as amended.

(U) DEFINITIONS

16. (U//~~FOUO~~) Non-releasable Information – NOFORN information or information that is releasable to a community of which the Second Party Integree is not a member (for example, REL US/UK information for a Canadian Integree).

17. (U) NSA/CSS Global Cryptologic Enterprise – NSA/CSS worldwide personnel, systems, and facilities:

a. (U) NSA/CSS Headquarters: Primary location of the NSA/CSS Senior Leadership Team.

b. (U) NSA/CSS Washington (NSAW): NSA/CSS facilities at the Fort Meade, FANX, and associated campuses [Finksburg, Kent Island, and all leased facilities in the Baltimore/Washington metropolitan area].

c. (U) NSA/CSS Extended Enterprise (Field): NSA/CSS personnel, systems, and facilities at locations other than NSAW. (Source: Corporate Glossary)

18. (U//~~FOUO~~) Raw SIGINT Data – Any SIGINT data acquired either as a result of search and development or targeted collection operations against a particular foreign intelligence target before the information has been minimized and evaluated for foreign intelligence purposes. (Source: Corporate Glossary)

19. (U//~~FOUO~~) Second Party – Any of the four countries with which the U.S. Government maintains SIGINT and IA relationships, namely the United Kingdom, Canada, Australia, and New Zealand.

20. (U//~~FOUO~~) Second Party Integrees – Second Party personnel integrated into an NSA/CSS or United States Cryptologic System element who, when integrated into an NSA/CSS environment, are working solely under the direction and operational control of the DIRNSA/CHCSS to conduct cryptologic or information assurance activities that support NSA/CSS mission in accordance with NSA/CSS authorities, rules, and regulations. Integrees may be civilian or military Second Party SIGINT or IA personnel but may not be contractors. Equivalent to the term Foreign Exchange Personnel: an individual from one of the Second Party cryptologic entities assigned to work for NSA/CSS under DIRNSA/CHCSS authorities. Duties associated with an Integree's position shall be performed in support of the NSA/CSS mission and in compliance with Executive Order 12333, "United States Intelligence Activities," as amended (Reference k).

21. (U//~~FOUO~~) Second Party Liaison – An individual representing one of the Second Party nations' SIGINT or IA counterpart organizations at NSA/CSS. Duties associated with this position will be performed primarily in support of the counterpart organization.